Workshop
Protection Profile Development

Contact Information

- Elizabeth Foreman(foreman@mitretek.org)

  Mitretek
  (703) 610-1658

- Gary Stoneburner (gary.stoneburner@nist.gov)

  NIST, Computer Security Division
  (301) 975-5394

Workshop Contents

- Background Information
- CC Presentation
- Protection Profile Development
  - Mini Threat Analysis Exercise
  - Security Objective Definition Exercise
  - Security Requirements Selection Exercise
  - Group Briefings
- Panel - Window into the Future
- Conclusions

At the end of this workshop, you will ...

- have a general understanding of the CC and know how to use it,
- be ~~an intermediate~~ a novice protection profile developer,
- understand how a protection profile is evaluated,
- know where to find more information.

Workshop Schedule
Tuesday

- 8am - 9am: Introduction
- 9am - 12pm: CC Presentation/Drills
- 12pm - 1pm: Lunch
- 1pm - 4pm: CC Presentation/Drills

Workshop Schedule
Wednesday

- 8am - 9am: Walk-through of a sample PP
- 9am - 10am: Threat Analysis Review
- 10am - noon: Mini-Threat Analysis Exercise
- 12pm - 1pm: Lunch
- 1pm - 2pm: Security Objectives Review
- 2pm - 4pm: Security Objective Development Exercise

Workshop Schedule
Thursday

- 8am - 9am: Requirements Review
- 9:00am - noon: Requirements Selection Exercise
- noon - 1pm: Lunch
- 1pm - 4pm: Continue Exercise and Prepare Briefings

Workshop Schedule
Friday

- 8am - 10am: Finish Preparing Briefings
- 10am - noon: Briefings & Discussion
- 12pm - 1pm: Lunch
- 1pm - 3pm: Panel - Window into the Future
- 3pm - 4pm: Comments from the Class

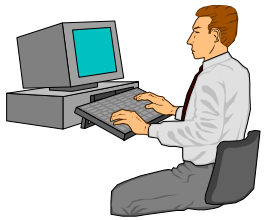
Scope of the Common Criteria

- Basis for evaluation of security properties of IT systems and products
- Allows independent evaluations to be compared
- Addresses protection of information from unauthorized disclosure, modification, or loss of use
- Applicable to IT security measures implemented in HW, SW, firmware

CC Intended Audience

- Consumers

- Developers



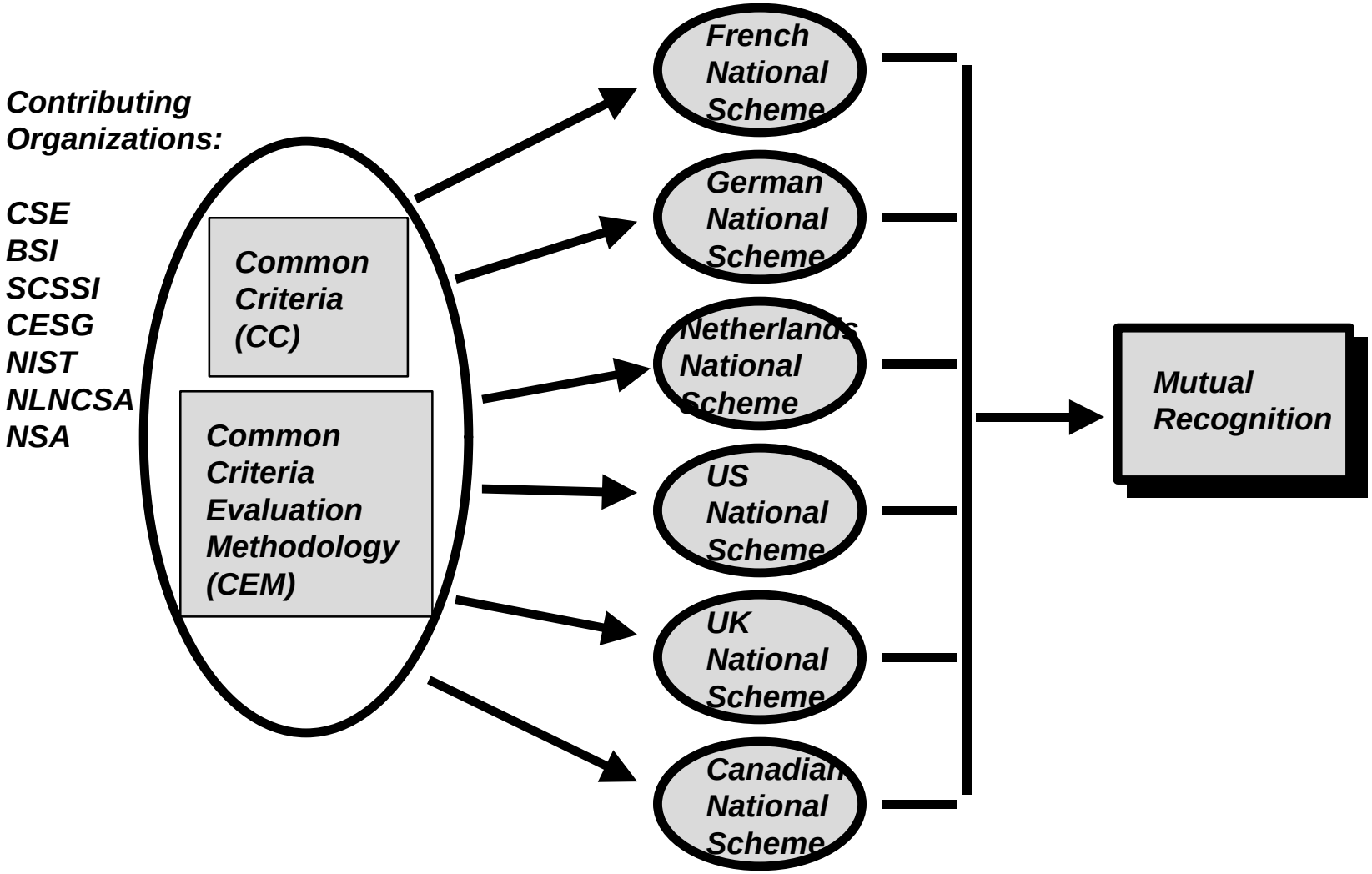
- Evaluators

- Others ...

The CC Does Not Address...

- ...administrative measures
- ...physical aspects of IT security
- ...evaluation methodology
- ...mutual recognition agreements
- ...cryptographic *algorithms*
- ...accreditation

The Big Picture



Common Criteria History

- TCSEC developed by U.S. in 1980s
- ITSEC developed by European Commission in 1991
- CTCPEC developed in Canada in 1993
- Federal Criteria (FC) drafted by U.S. in 1993
- CC Version 1.0 available 1/96
- CC Version 2.0 available 5/98

CC Committees

- CCEB - drafted Version 1.0, solicited and responded to reviewer comments
- CCIB - dealt with issues, comments, responsible for Version 2.0
- CCIMB - responsible for interpretations of Version 2.0

The CC vs. The OB

- The TCSEC states criteria for several sets of functional and assurance requirements (e.g., C2, B1)
- The CC provides a *catalog* of criteria for stating functional and assurance requirements

Summary: What is the Common Criteria?

- The CC is a catalog of criteria and a set of tools for construction of requirements
- These requirements serve as a
  - ... guide for the development of products with IT security features
  - ... guide for the procurement of products with IT security features
  - ... basis for the evaluation of IT security products

Terminology Drill

Terminology Drill - Answers

1) TOE i
2) IT t
3) Security Target h
4) TSF j
5) Family e
6) Package a
7) Protection Profile n
8) TSP p
9) Trusted Path c
10) Role m
11) Class d
12) Reference Monitor s

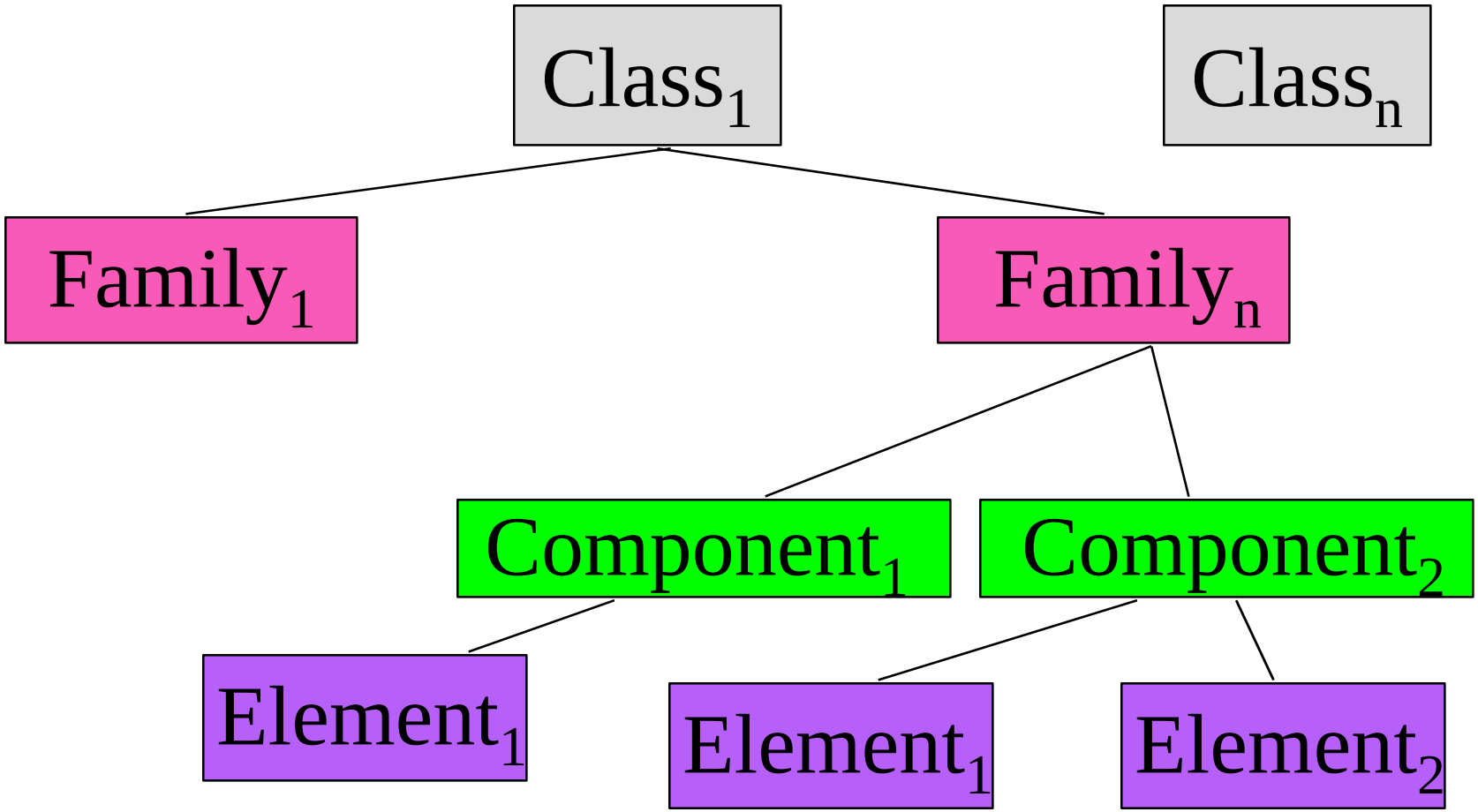
CC Look & Feel

- Part 1: Introduction and General Model
- Part 2: Security Functional Requirements
- Part 2: Annexes
- Part 3: Security Assurance Requirements

CC Part 1:
Introduction & General Model

- Scope, Glossary, Overview
- Security Context & CC Approach
- Security Concepts, Environment & Objectives
- Evaluation Results
- Appendix A: History
- Appendix B&C: Specification of PPs & STs

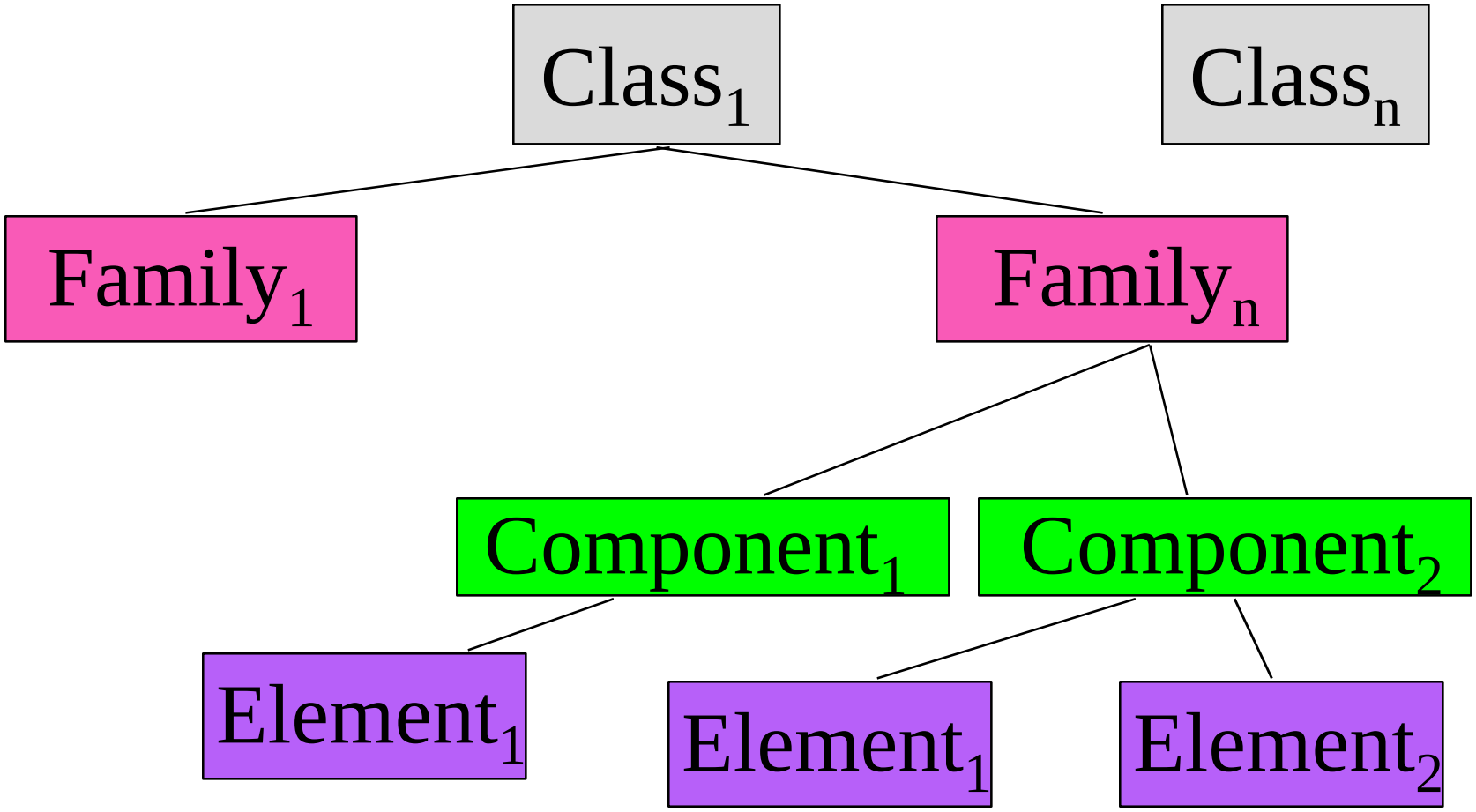
CC Part 2:
Security Functional Requirements



CC Part 2: Annexes

- Annex A: Security Functional Requirements Application Notes
  - Dependency Table
- Annex B - M: Similar to Part 2 but more informative
  - user notes
  - evaluator notes
  - documentation notes

CC Part 3:
Security Assurance Requirements



CC Part 1:
Introduction & General Model

- *ALL TOE security requirements ultimately arise from consideration of the purpose and context of the TOE.*
- This definition requires the PP or ST writer to describe the security needs to be addressed and refine this general description into a specific description of the *security environment*, which leads to a statement of *security objectives*.

Establishing a Security Environment

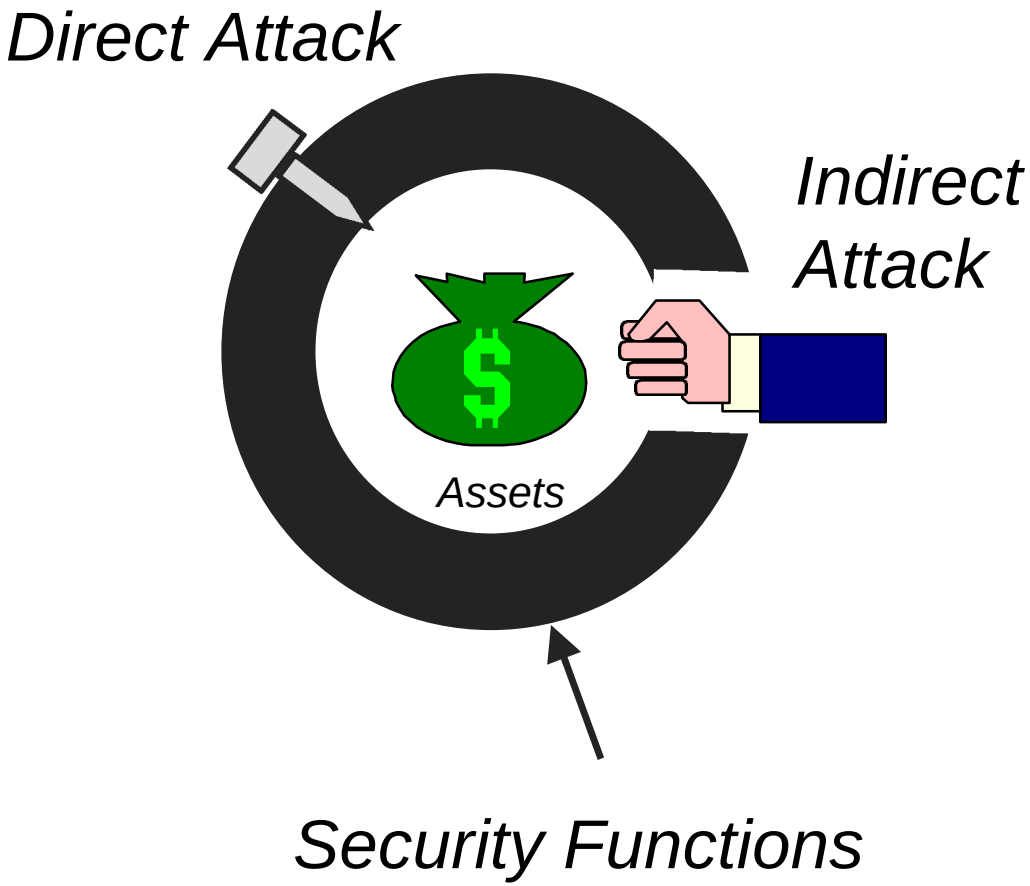
Consider:

- TOE physical environment
- Assets requiring protection
- TOE purpose

TOE Security Environment

- Secure Usage Assumptions
- Threats
- Organizational Security Policies

Simple Example



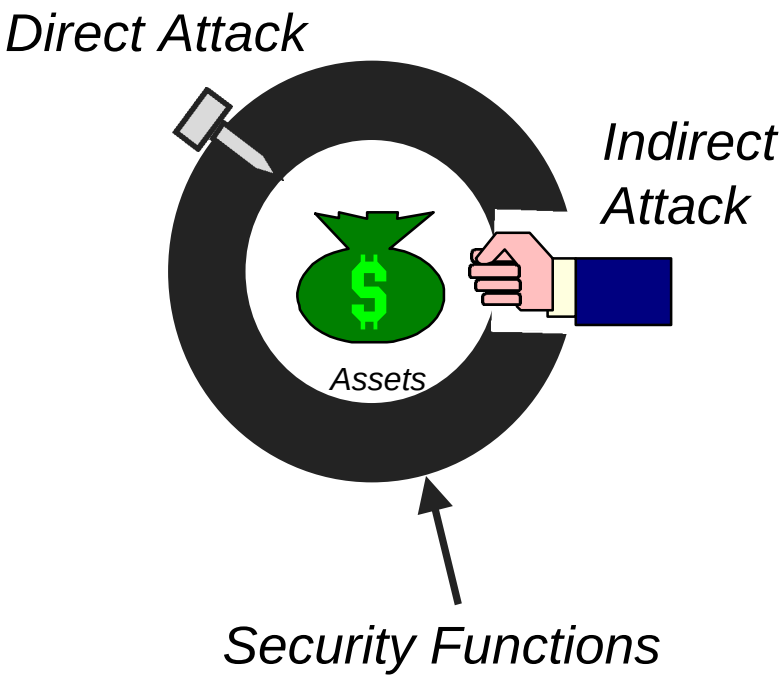
Secure Usage Assumptions

Identifies the significant assumptions made in the development of this PP; for example, security aspects of the environment in which the TOE will be used and how the TOE is to be used within this environment.

- Information about environment:
  - physical issues
  - connectivity issues
  - personnel issues
- Information about intended usage:
  - intended application
  - potential asset value
  - possible usage limitations

Example Secure Usage Assumptions

- A.PROTECT The wall is intended to protect real property small enough to fit inside the wall and valued under one million dollars.
- A.PHYSICAL The wall is physically protected by a moat.
- A.SINGLE The wall is located in a separate building and is not connected to any other part of the facility.
- A.NO_EVIL All employees and wall developers are trustworthy.



Threat Analysis

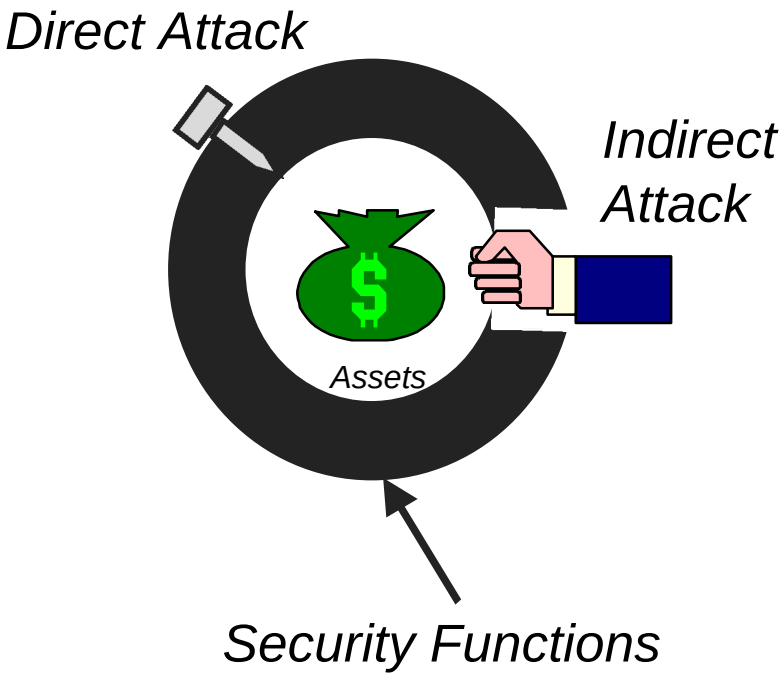
- Threat Agent

- The Attack

- Assets

THREATS

- T.DIRECT An attacker penetrates the protective wall and steals the assets (direct attack).
- T.INDIRECT An attacker takes advantage of a flaw in the design of the protective wall and steals the assets (indirect attack).
- T.DESTROY An attacker destroys the protective wall via explosives, fire, etc., and steals the assets (direct attack).



Security Policies

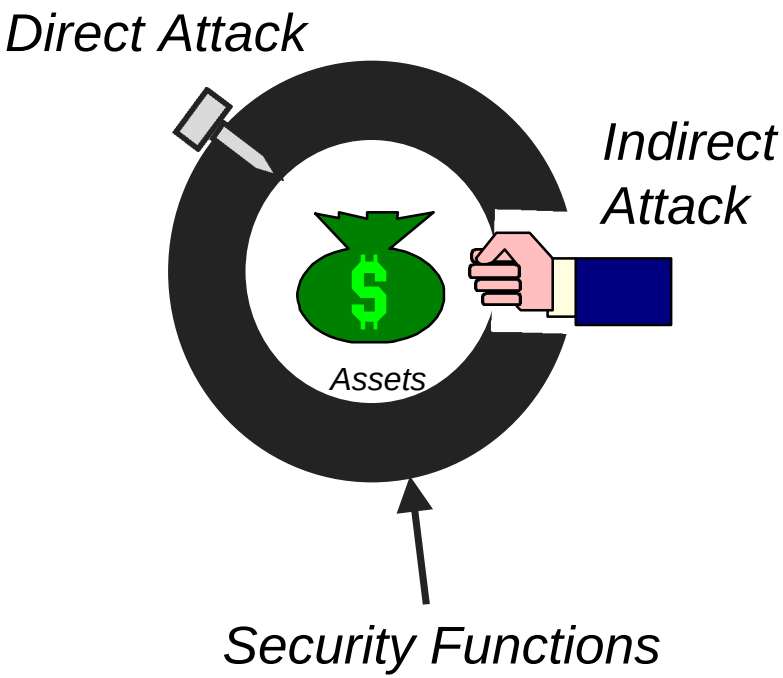
- Security Function Policy (SFP)
- TOE Security Policy (TSP)

- Organizational Security Policy:

  A set of rules, procedures, practices, or guidelines imposed by an organization upon its operations and to which the TOE may have to comply.

Example Organizational Security Policies

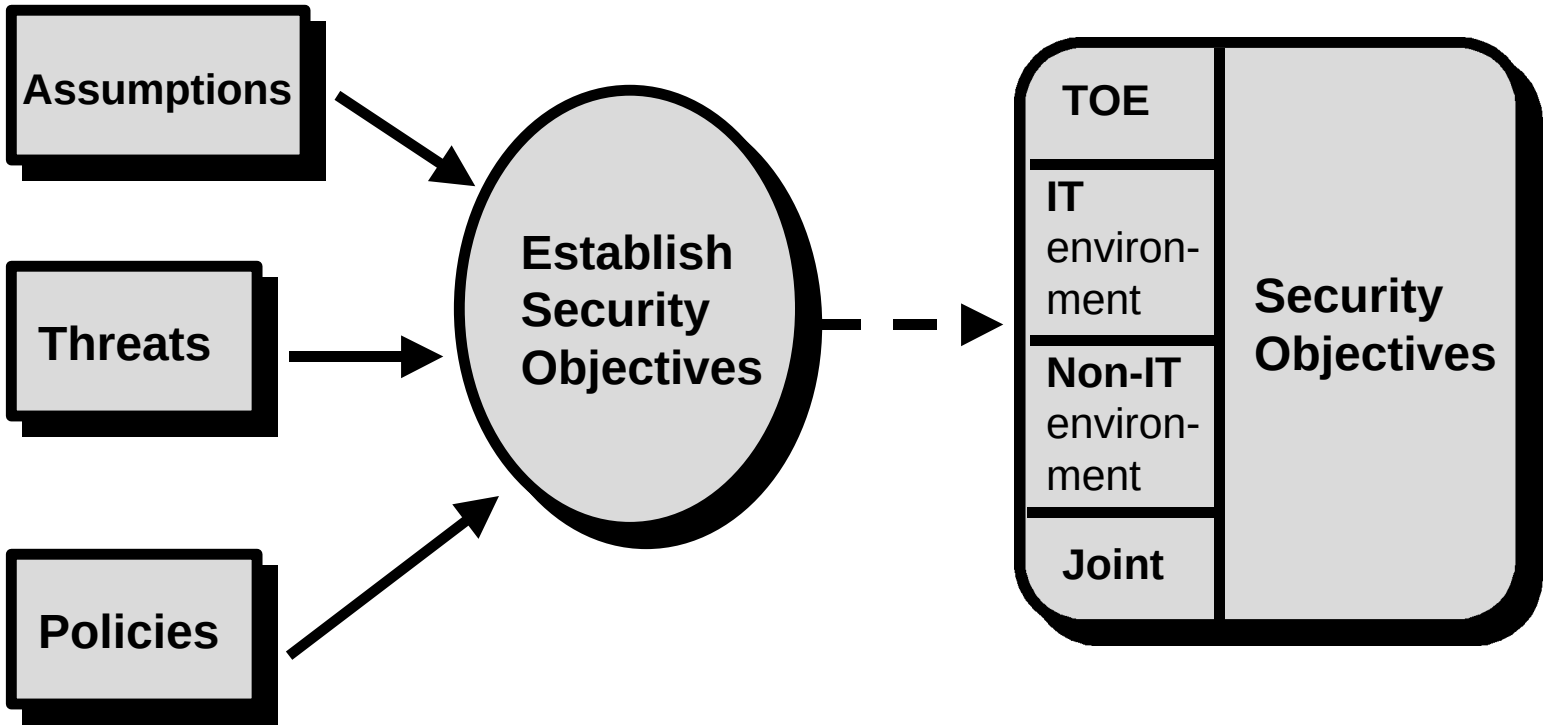
- **P.TRAIN** All individuals who access the wall receive training in proper use.
- **P.MANUAL** There must be a manual means for protecting the assets if the wall becomes unusable.



Mapping Table

Security Environment	Security Objectives
T.DIRECT	
T.INDIRECT	
T.DESTROY	
A.PHYSICAL	
A.SINGLE	
A.NO_EVIL	
P.TRAIN	
P.MANUAL	

Security Objective Development



Security Objectives reflect the intent to counter identified threats and/or address any identified organizational security policies and assumptions.

Types of Security Objectives

- Security Objectives for the TOE
  - *Addressed by the TOE*
  - *Environmental support general in nature*
- Security Objectives for the environment
  - *IT: Addressed by IT other than the TOE*
  - *Non-IT: Addressed by non-technical and procedural means*
- Joint Security Objectives
  - *Addressed by the TOE and environment*
  - *Environmental support specific in nature*

Mapping Table

Security Environment	Security Objectives
Security Objectives for the TOE	
T.DIRECT	
T.INDIRECT	
T.DESTROY	
A.PHYSICAL	
Security Objectives for the Environment	
T.DESTROY	
A.PHYSICAL	
A.SINGLE	
A.NO_EVIL	
P.TRAIN	
P.MANUAL	

Security Objectives for the TOE

- **O.DIRECT** The protective wall must be thick enough to prevent direct attacks.
- **O.INDIRECT** The protective wall must not contain any obvious flaws in design or implementation.
- **O.PHYSICAL** Those responsible for the TOE must ensure that those parts of the TOE critical to the security policy are protected from physical attack.

Security Objectives for the Environment

- **O.INSTALL** Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.
- **O.SINGLE** Those responsible for the TOE must ensure that the TOE is installed in a stand-alone manner and is not part of a network.
- **O.TRAIN** Those responsible for organizational security must provide initial and ongoing security awareness training.
- **O.MANUAL** An alternative means exists for securing the assets if the wall becomes unusable, and administrators know the procedures.

Completed Mapping Table

Security Environment	Security Objectives
Security Objectives for the TOE	
T.DIRECT	O.DIRECT
T.INDIRECT	O.INDIRECT
T.DESTROY	O.PHYSICAL
A.PHYSICAL	O.PHYSICAL
Security Objectives for the Environment	
T.DESTROY	O.INSTALL
A.PHYSICAL	O.INSTALL
A.SINGLE	O.SINGLE, O.INSTALL
A.NO_EVIL	O.TRAIN
P.TRAIN	O.TRAIN
P.MANUAL	O.MANUAL

CC General Model Terminology

- Secure Usage Assumptions

  Assumptions used in the production of the PP, including the security aspects of the TOE's environment and how the TOE will be used in that environment.

- Threats

  The intentional exploitation or unintentional triggering of a vulnerability by a threat-agent (individual or event).

- Organizational Security Policy

  A set of rules, procedures, practices, or guidelines imposed by an organization upon its operations and with which the TOE must comply.

- Security Objective

  Security Objectives provide information on how the PP will, in light of the stated assumptions, counter the identified threats and meet the identified organizational security policies.

Procedure for Identifying Security Environment & Objectives

① **Identify Secure Usage Assumptions by investigating the TOE operating environment particularly the intended usage and the physical environment.**

① **Conduct a Threat Analysis and/or refer to any known threats.**

③ **Identify any Organizational Security Policies.**

④ **Develop Security Objectives to counter threats or support policies and assumptions.**

° **Categorize Security Objectives by type (may be more than one)**

± **Verify:**

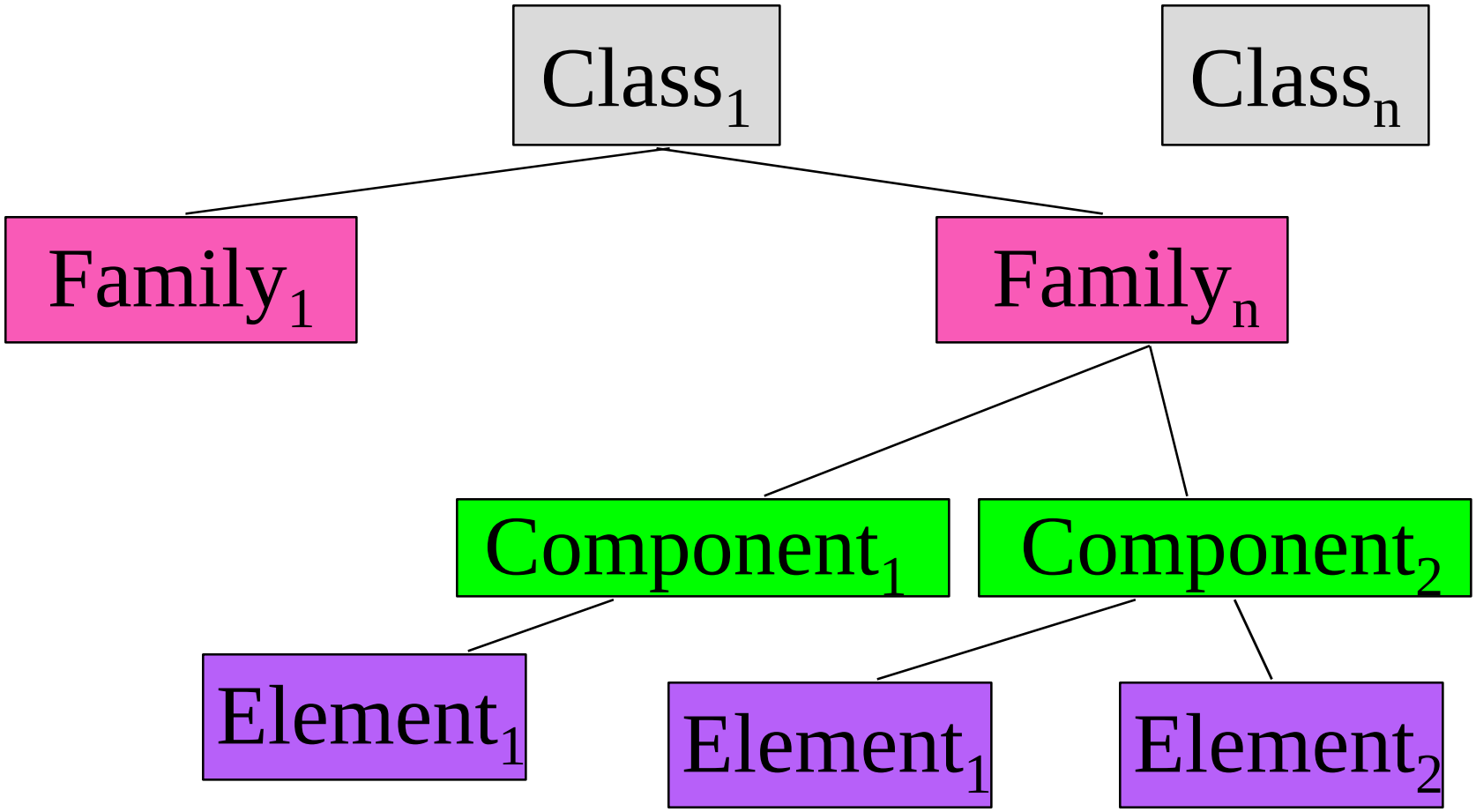
- **that objectives do not conflict with any policies or assumptions**
- **that objectives do not conflict with each other**
- **that all threats, policies and assumptions addressed**

⑦ **Repeat steps 4-6 until all inconsistencies resolved.**

Security Functional Requirements

Levied upon functions of the TOE that support IT security; their behavior can generally be observed

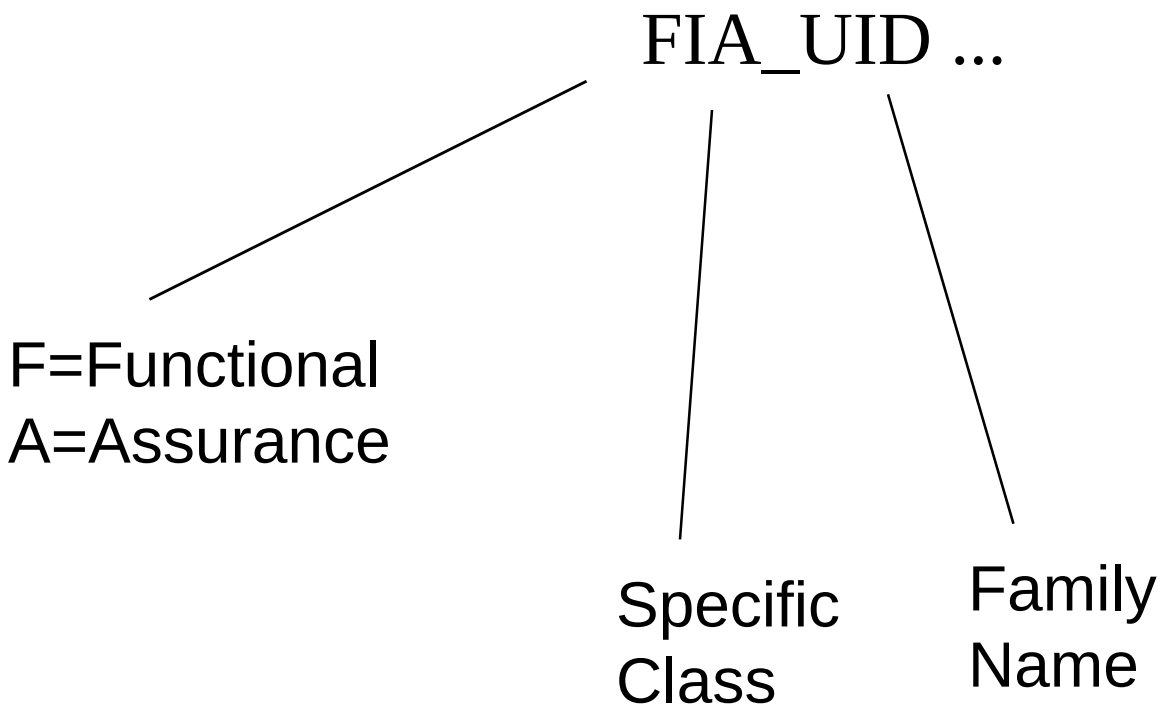
CC Part 2:
Security Functional Requirements



Definitions

- Class - for organizational purposes; all members share a common focus
- Family - for organizational purposes; all members share security objectives but may differ in emphasis
- Component - describes an actual set of security requirements; smallest selectable set
- Element - members of a component; cannot be selected individually

Functional Requirement Names



FIA_UID User Identification

Family behavior

This family defines the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification.

Component leveling

FIA_UID.1 Timing of identification, allows users to perform certain actions before being identified by the TSF.

FIA_UID.2 User identification before any action, require that users identify themselves before any action will be allowed by the TSF.

FIA_UID User Identification (cont.)

Management: FIA_UID.1

The following actions should be considered for the management functions in FMT:

a) the management of the user identities;

b) if an authorized administrator can change the actions allowed before identification, the managing of the action lists.

Management: FIA_UID.2

The following actions should be considered for the management functions in FMT:

a) the management of the user identities.

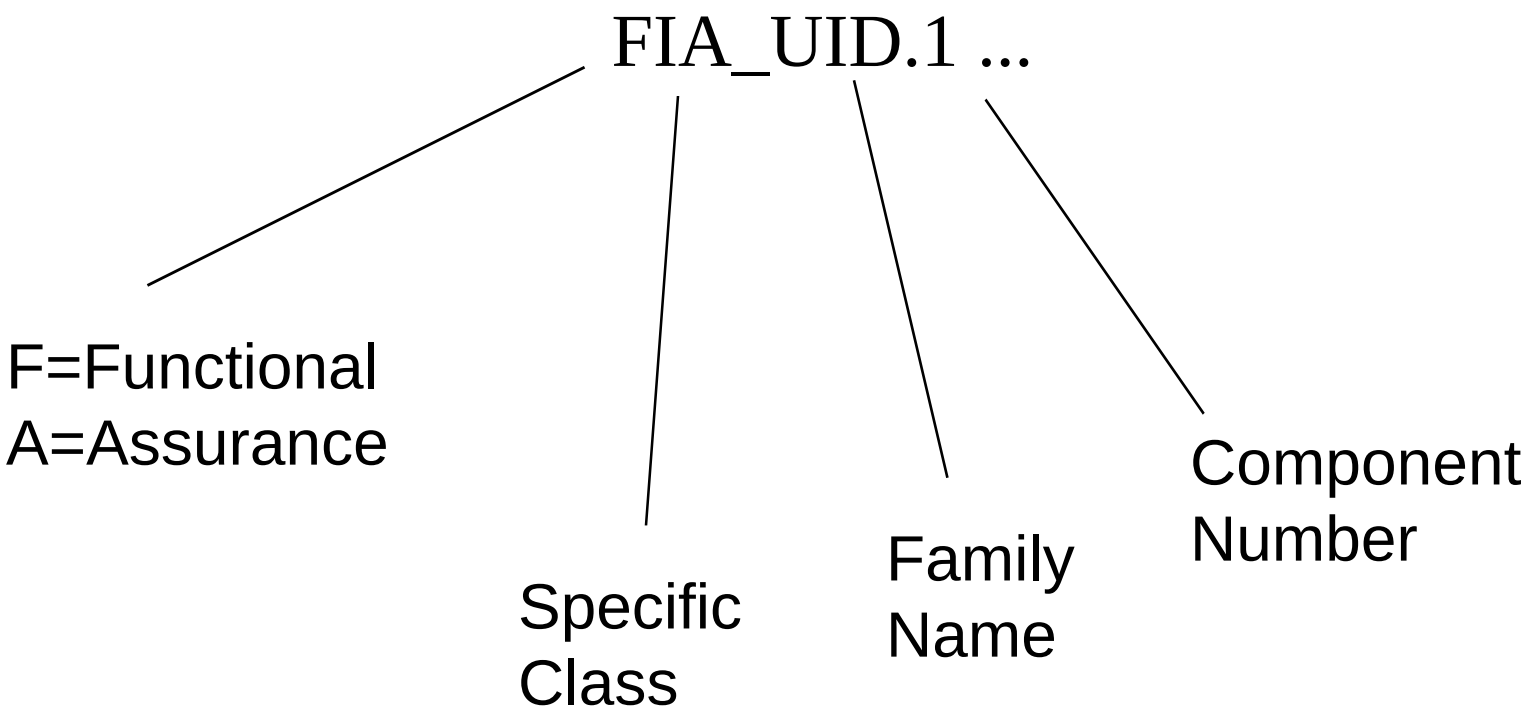
Audit:FIA_UID.1, FIA_UID.2

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

a) Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided.

b) Basic: All use of the user identification mechanism, including the user identity provided.

Interpreting Functional Requirement Names



FIA_UID.1 Timing of Identification

Hierarchical to: no other components.

FIA_UID.1.1 **The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.**

FIA_UID.1.2 **The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.**

Dependencies: **No dependencies**

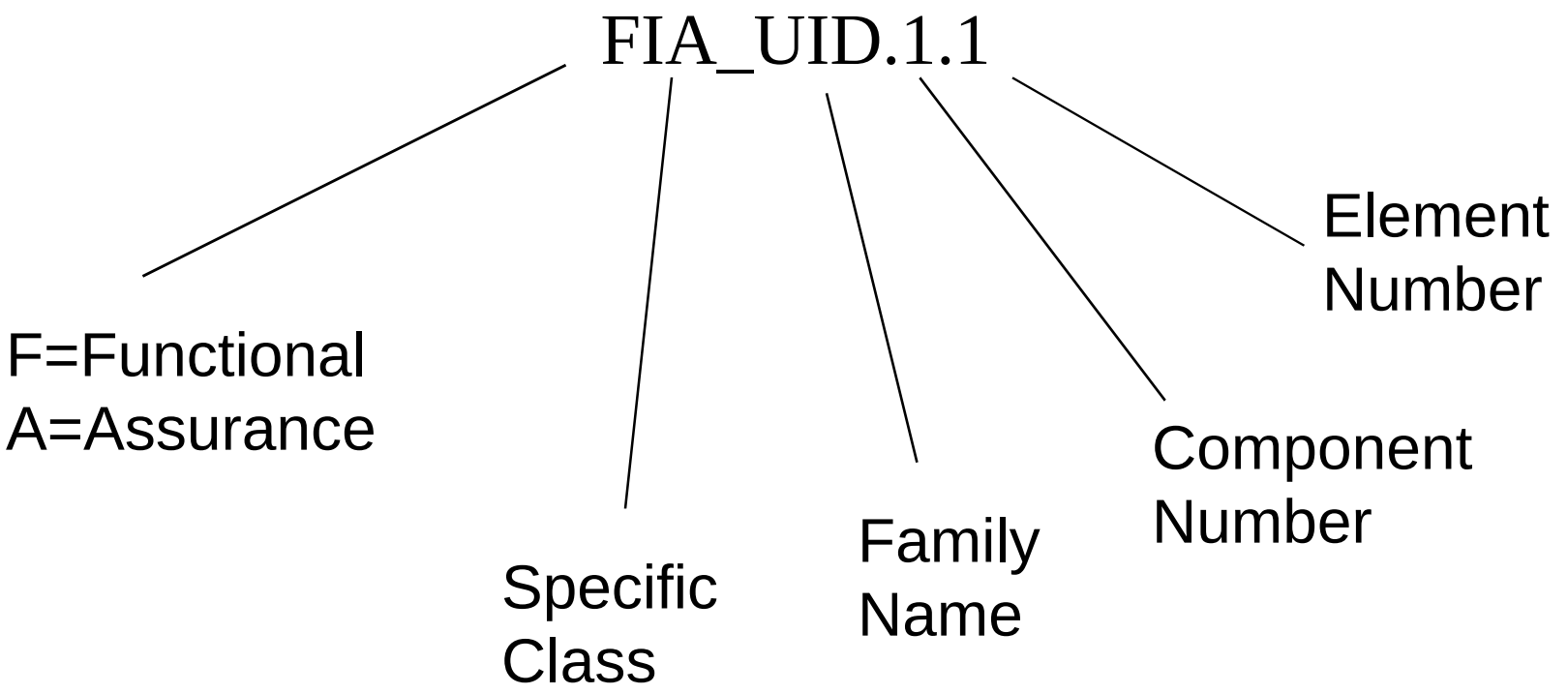
FIA_UID.2 User Identification before any action

Hierarchical to: FIA.UID.1

FIA_UID.2.1 **The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.**
resides in the TOE.

Dependencies: **No dependencies**

Interpreting Functional Requirement Names



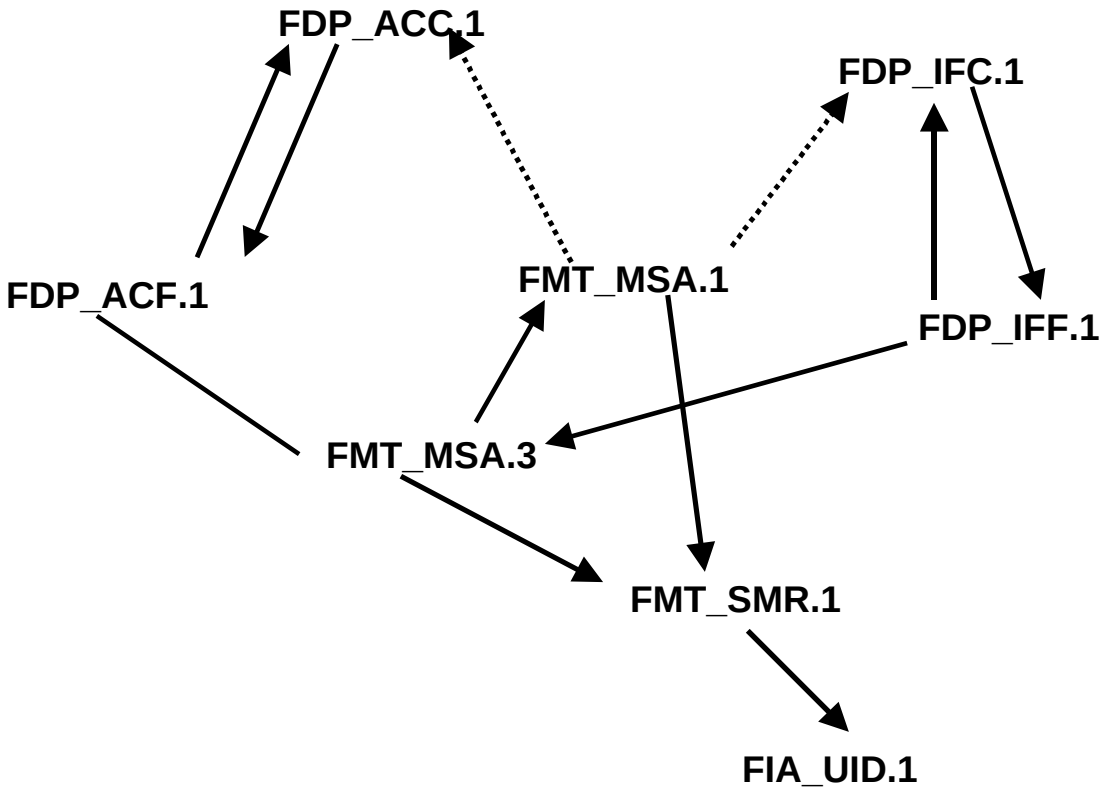
Find the Requirement Drill

Dependencies

- Some requirement components are not self sufficient
- Some functional requirement components have functional and/or assurance dependencies
- Dependent components may be eliminated with rationale - “soft dependencies”

Chasing Dependencies - Method 1

Example - FDP_ACF.1



Chasing Dependencies - Method 2

Security Functional Requirement	Dependencies
FDP_ACF.1	FDP_ACC.1
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1 FMT_SMR.1
...	...

Operations on Requirements

- Selection
- Assignment
- Refinement
- Iteration

Selection Operation

- Specification of elements selected from a list given in the component
- “Multiple Choice” operation
- Allows PP/ST writer to select from a provided list of choices

Selection Operation Example

As Written in the Common Criteria:

- **FAU_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

  a) Start-up and shutdown of the audit functions;

  b) All auditable events for the [selection: *minimum*, *basic*, *detailed*, *not specified*] level of audit; and ...

After Selection Operation:

- **FAU_GEN.1.1** The TSF shall be able to generate an audit record of the following auditable events:

  a) Start-up and shutdown of the audit functions;

  b) All auditable events for the [selection: *minimum*] level of audit; and ...

Assignment Operation

- Specification of a parameter filled in when component is used
- “Fill in the Blank” operation
- Allows PP/ST writer to provide information relating to application of the requirement

Assignment Operation Example

As Written in the Common Criteria:

- **FMT_SMR.1.1** The TSF shall maintain the roles: [assignment: *the authorized identified roles*].

After Assignment Operation:

- **FMT_SMR.1.1** The TSF shall maintain the roles: [assignment: *authorized administrator*, *security officer*, *operator*].

Refinement Operation

- Addition of detail to component
- Allows PP/ST writer to specify additional detail to ***narrow*** the scope of a functional requirement

Refinement Operation Example

As Written in the Common Criteria:

- **FAU_SAA.1.1** The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

After Refinement Operation:

- **FAU_SAA.1.1** The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP by notifying the Security Officer immediately.

Iteration Operation

- Repetitive use of the same requirement to address different aspects (e.g., identification of more than one type of user)

Iteration Operation Example

As Written in the Common Criteria:

- **FMT_MTD.1.1** The TSF shall restrict the ability to [selection: *change_default*, *query*, *modify*, *delete*, *clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorized identified roles*].

After Iteration Operation:

- **FMT_MTD.1.1** The TSF shall restrict the ability to [selection: *modify*] the [assignment: *enrolled images db*] to [assignment: *the authorized administrator*].
- **FMT_MTD.1.1** The TSF shall restrict the ability to backup/restore the enrolled images db to the authorized operator.

Operations Drill

The 11 Security Functional Classes

- Security Audit (FAU)
- Communications (FCO)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Identification & Authentication (FIA)
- Security Management (FMT)
- Privacy (FPR)
- Protection of the TOE Security Functions (FPT)
- Resource Utilization (FRU)
- TOE Access (FTA)
- Trusted Path (FTP)

Class FAU: Security Audit

- Common Intent: All of the 6 families in this class are concerned with ...
  - recognizing (FAU_ARP)
  - recording (FAU_GEN, FAU_SEL)
  - storing (FAU_STG)
  - analyzing (FAU_SAA, FAU_SAR)

... security-relevant events and activities.

Class FAU: Security Audit
Example

NEED: A record of certain actions taken by users such that an administrator can determine when the action occurred, who did it, whether it succeeded or failed.

TO SATISFY:

FAU_GEN.1 Audit Data Generation

FAU_GEN.2 User Identity Association

Class FCO: Communication

- Common Intent: The 2 families in this class are concerned with ...
  - proof of origin (FCO_NRO)
  - proof of receipt (FCO_NRR)

... of transmitted information.

Class FCO: Communication Example

NEED: The recipient of all email messages must be able to verify the identity of the sender.

TO SATISFY:

FCO_NRO.1 Selective Proof of Origin

FCO_NRO.2 Enforced Proof of Origin (more functionality)

Class FCS: Cryptographic Support

- Common Intent: The 2 families in this class are concerned with ...
  - management (FCS_CKM)
  - operation (FCS_COP)

... of cryptographic keys.

Class FCS: Cryptographic support Example

NEED: An administrator must generate and distribute cryptographic keys according to the appropriate algorithms and distribution, respectively.

TO SATISFY:

FCS_CKM.1 Cryptographic Key Generation

FCS_CKM.2 Cryptographic Key Distribution

Class FDP: User Data Protection

- Common Intent: The 13 families in this class are concerned with ...
  - security function policies (FDP_ACC, FDP_IFC)
  - forms of user data protection (FDP_ACF, FDP_IFF, FDP_ITT, FDP_RIP,FDP_ROL, FDP_SDI)
  - import/export (FDP_DAU, FDP_ETC, FDP_ITC)
  - inter-TSF communications (FDP_UCT, FDP_UIT)

... for data protection.

Class FDP: User Data Protection Example

NEED: When a user data file is deleted its contents must be inaccessible and when a new one is created it should contain no previous information.

TO SATISFY:

FDP_RIP.2 Full Residual Information Protection

Class FIA: Identification & Authentication

- Common Intent: The 6 families in this class are concerned with ...
  - establishing (FIA_AFL, FIA_ATD, FIA_SOS, FIA_USB)
  - verifying (FIA_UAU, FIA_UID)

... claimed user identity.

Class FIA: Identification & Authentication Example

NEED: An individual may only attempt to log into the system 3 times. After that, if the attempts are not successful, the individual's account shall be locked until unlocked by an administrator.

TO SATISFY:

FIA_AFL.1 Basic Failure Handling

Class FMT: Security Management

- Common Intent: The 6 families in this class are concerned with ...
  - management of TSF data (FMT_MTD)
  - management of security attributes (FMT_MSA, FMT_REV, FMT_SAE)
  - management of the security functions (FMT_MOF)
  - security roles (FMT_SMR)

... of the TOE.

Class FMT: Security Management Example

NEED: Our organization has a security officer responsible for new users and I&A functions; and an audit administrator responsible for the audit mechanism.

TO SATISFY:

FMT_SMR.1 Security Management Roles

FMT_MOF.1 Management of Functions in TSF

Class FPR: Privacy

- Common Intent: The 4 families in this class are concerned with protection against ...
  - discovery and misuse (FPR_ANO, FPR_PSE, FPR_UNL, FPR_UNO)

... of an individual's identity by others.

Class FPR: Privacy Example

NEED: There are a number of sensitive data files stored in a specific directory. It is important that only an administrator be able to determine if/when and by whom those data files are manipulated.

TO SATISFY:

FPR_UNO.1 Unobservability

Class FPT: Protection of the Trusted Security Functions

- Common Intent: The 16 families in this class are concerned with ...
  - protection (FPT_PHP, FPT_AMT, FPT_TST, FPT_SEP, FPT_RVM, FPT_RCV, FPT_FLS, FPT_TRC, FPT_ITA, FPT_ITC, FPT_ITI, FPT_ITT, FPT_RPL, FPT_SSP, FPT_STM)
  - management (FPT_TDC)

... of the TSF mechanisms and data.

Class FPT: Protection of the Trusted Security Functions Example

NEED: An authorized administrator must be able to verify that the executables that implement the security functions have not been modified by malicious individuals or code.

TO SATISFY:

FPT_TST.1 TSF Self Test

Class FRU: Resource Utilization

- Common Intent: The 3 families in this class are concerned with ...
  - availability (FRU_FLT)
  - allocation (FRU_PRS, FRU_RSA)

... of resources.

Class FRU: Resource Utilization Example

NEED: Since only one printer is available, its use must be allocated first to higher-priority tasks.

TO SATISFY:

FRU_PRS.1 Limited Priority of Service

Class FTA: TOE Access

- Common Intent: The 6 families in this class are concerned with ...
  - attributes (FTA_LSA, FTA_TAB, FTA_TAH)
  - establishment (FTA_MCS, FTA_SSL, FTA_TSE)

... of a user session.

Class FTA: TOE Access Example

NEED: Whenever a user session remains idle for a specified period of time, the session shall be automatically locked by the system. Also, individuals shall have the ability to lock their own sessions.

TO SATISFY:

FTA_SSL.1 TSF-Initiated Locking

FTA_SSL.2 User-Initiated Locking

Class FTP: Trusted Path/Channels

- Common Intent: The 2 families in this class are concerned with ...
  - trusted communication paths (FTP_TRP)
  - trusted communication channels (FTP_ITC)

... between users and the TSF; and between the TSF and other trusted IT products.

Class FTP: Trusted Path/Channel Example

NEED: There must be a means by which an individual can verify that they are communicating with the TSF.

TO SATISFY:

FTP_TRP.1 Trusted Path

Functional Requirements Drill

Functional Requirements Rationale

- **Security objectives drive functional requirement selection!!**
- Rationale must demonstrate that the functional requirements are ***suitable to meet and traceable to*** the security objectives
- The Rationale must demonstrate:
  - functional & assurance requirements together meet the security objectives
  - security requirements together form a mutually supportive and internally consistent whole
  - the choice of security requirements is justified
  - strength of function (SOF) claims are consistent with the security objectives

Class FAU: Security Audit

- Common Intent: All of the 6 families in this class are concerned with ...
  - recognizing (FAU_ARP)
  - recording (**FAU_GEN**, FAU_SEL)
  - storing (FAU_STG)
  - analyzing (FAU_SAA, FAU_SAR)

... security-relevant events and activities.

FAU_GEN.1 Audit Data Generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and Shutdown of the audit functions;

b) All auditable events for the [selection: *minimum*, *basic*, *detailed*, *not specified*] level of audit; and

c) [assignment: *other specifically defined auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment; *other audit relevant information*].

Audit Generation Example

FIA_UAU.1 Timing of Authentication

AUDIT:

The following actions should be auditable if FAU_GEN Security Audit Data Generation is included in the PP/ST:

a) Minimal: Unsuccessful use of the authentication mechanism.

b) Basic: All use of the authentication mechanism.

c) Detailed: All TSF mediated actions performed before authentication of the user.

FAU_GEN.1.1(a): “minimal” level chosen

Auditable Event	Motivated by Requirement
Any unsuccessful use of the authentication mechanism.	FIA_UAU.1 Timing Of Authentication
Rejection of requests to initiate a session based on the limitation of multiple concurrent sessions.	FTA_MCS.1 Basic Limitation on Multiple Concurrent Sessions

FAU_GEN.1.1(a): “basic” level chosen

Auditable Event	**Motivated by Requirement**
All use of the authentication mechanism.	FIA_UAU.1 Timing Of Authentication
No change, same as minimal.	FTA_MCS.1 Basic Limitation on Multiple Concurrent Sessions

FAU_GEN.1.1(a): “detailed” level chosen

Auditable Event	Motivated by Requirement
All TSF mediated actions performed by a user prior to authentication.	FIA_UAU.1 Timing Of Authentication
The audit record shall include the number of concurrent sessions and the user’s security attributes.	FTA_MCS.1 Basic Limitation on Multiple Concurrent Sessions

FAU_GEN.1.1(a): “not specified” chosen

Auditable Event	Motivated by Requirement
Only successful use of the authentication mechanism shall be recorded in the audit trail.	FIA_UAU.1 Timing Of Authentication
Successful requests to initiate a session, when a session already exists.	FTA_MCS.1 Basic Limitation on Multiple Concurrent Sessions

Audit Drill

Management

- Information for the PP/ST writer to consider as management activities for a given component
- The management activities are defined in requirements in the FMT class
- Informative only

Management Example

Management: FIA_UAU.2

The following actions should be considered for the management functions in FMT:

a) management of the authentication data by an administrator;

b) management of the authentication data by the user associated with this data.

FMTD.1.1 The TSF shall restrict the ability to [selection: *initialize*, *query*, *modify*, *delete*, *or clear*] the [assignment: *enrolled images database*, *i.e.*, *identifying name or number*, *physical or behavioral characteristic*, *role*] and [assignment: *any other enrolled images database attributes specific to the particular Biometric Device to be defined by the ST writer*] to [assignment: *authorized administrators*].

CC Part 3: Security Assurance Requirements

Why Do We Care About Assurance?

Answer - IT can be risky!

- **Threat-agents (human or event)**
  - Human or Event
  - Intentionally exploit or unintentionally trigger
- **Vulnerabilities**
  - Insufficient or incorrect requirements
  - Errors in design or implementation
  - Inadequate controls on operations

What is Assurance?

CC Definition:

Grounds for confidence that an entity meets its security objectives.

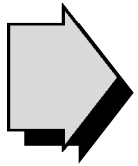
How Do We Gain Assurance?

One way is *Evaluation*

- Analysis of processes and procedures
- Checking that processes and procedures are being applied
- Analysis of the correspondence between TOE design representations
- Analysis of the TOE design representations against the requirements
- Verification of mathematical proofs
- Analysis of guidance documents
- Analysis of functional tests and results
- Independent functional testing
- Analysis for flaws
- Penetration testing

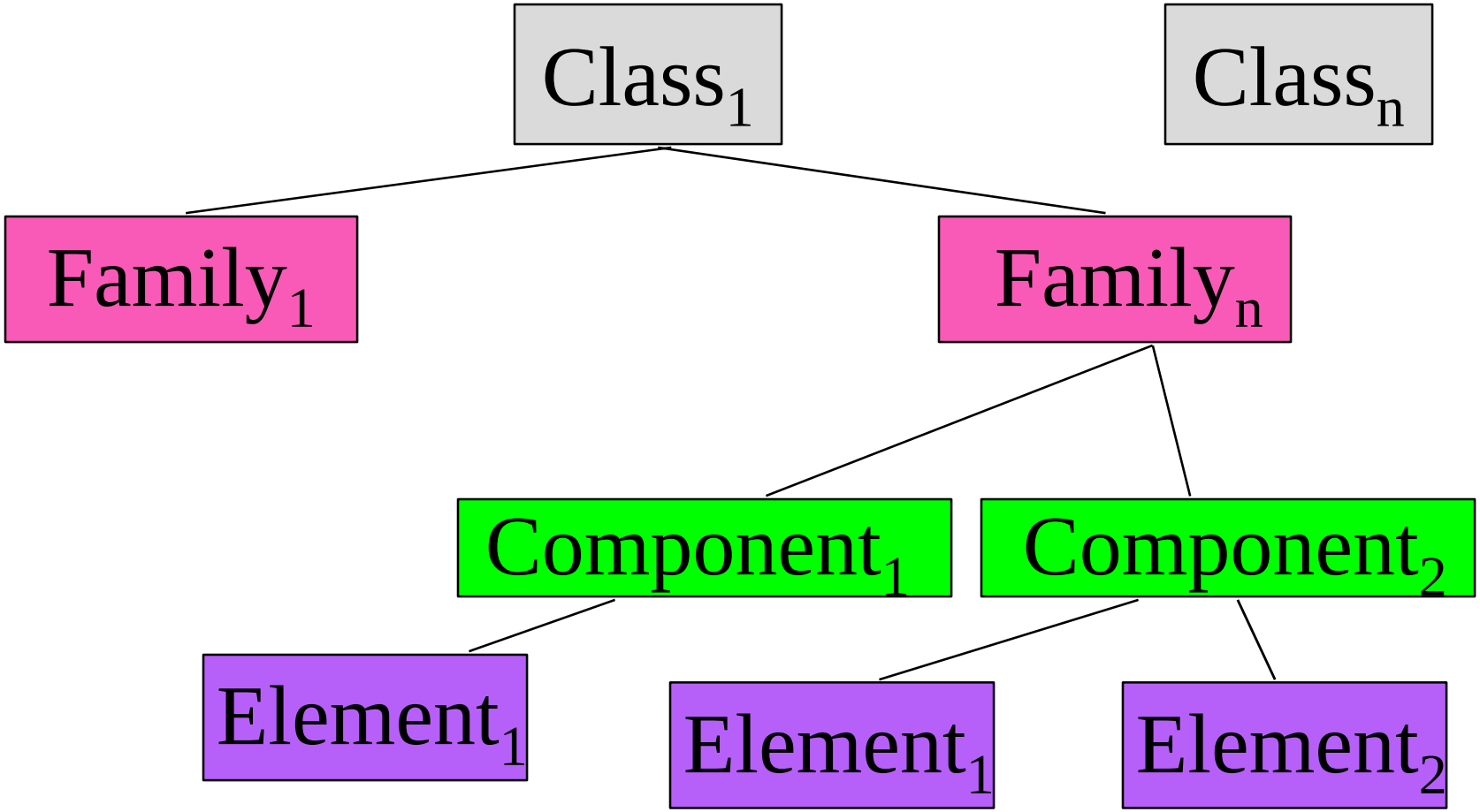
Evaluation Assurance Scale

Greater Evaluation Effort
(Scope, Depth, Rigor)

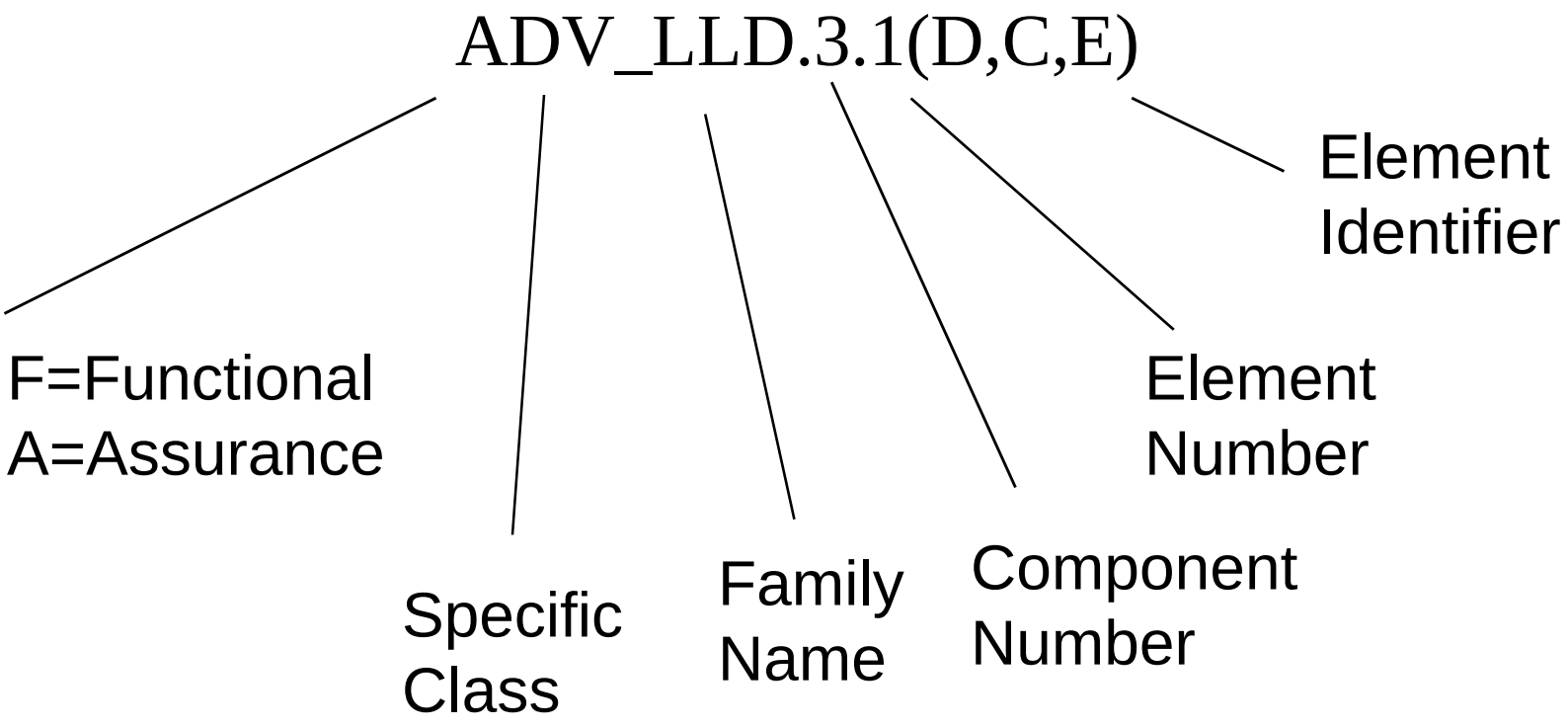


Greater
Assurance

Security Assurance Requirements Structure



Interpreting Assurance Requirement Names



Operations on Assurance Requirements

- Iteration
- Refinement
- Augmentation

Security
Assurance Classes

- Configuration Management (ACM)
- Delivery and operation (ADO)
- Development (ADV)
- Guidance documents (AGD)
- Life Cycle Support (ALC)
- Maintenance of Assurance (AMA)
- Tests (ATE)
- Vulnerability assessment (AVA)
- Evaluation Criteria (APE,ASE)

Class ACM: Configuration Management

- The 3 families in this class are concerned with ...
  - Specifying how much to control (SCP)
  - Specifying what controls are needed (AUT, CAP)

... of configuration items.

Class ADO: Delivery and Operation

- The 2 families in this class are concerned with ...
  - delivery (DEL)
  - installation, generation, start-up (IGS)

... of the TOE.

Class ADV: Development

- The 7 families in this class are concerned with ...
  - levels of abstraction (FSP, HLD, IMP, LLD)
  - correspondence mapping of representations (RCR)
  - internal structure (INT)
  - policy model (SPM)

... of the TSF.

Class AGD: Guidance Documents

- The 2 families in this class are concerned with ...
  - user (USR)
  - administrator (ADM)

... guidance documentation.

Class ALC: Life Cycle Support

- The 4 families in this class are concerned with refinement of the TOE during ...
  - development (DVS)
  - maintenance (FLR, LCD, TAT)

... phases.

Class AMA: Maintenance of Assurance

- The 4 families in this class are concerned with...
  - maintenance planning & procedures (AMP, EVD)
  - maintenance activities (CAT, SIA)

... after a TOE has been certified against the CC.

Class ATE: Tests

- The 4 families in this class are concerned with ...
  - coverage (COV)
  - depth (DPT)
  - nature of the testing to be performed (FUN, IND)

... testing.

Class AVA: Vulnerability Assessment

- The 4 families in this class are concerned with ...
  - exploitable covert channels (CCA)
  - misuse (MSU)
  - vulnerabilities and strength (VLA, SOF)

... of the TOE.

Assurance Component Dependencies

- Same concept as for functional requirements
- Table A.1 (Part 3: Annex A page 209) identifies "all" dependencies, both:
  - direct (as stated in the requirement)
  - indirect (as a result of "chasing down" the dependencies)
- Like functional dependencies, all are "soft"

Assurance Packages

- Reusable set of functional or assurance components combined together to satisfy a set of identified security objectives
- Currently, there are 7 assurance packages called Evaluation Assurance Levels (EAL1 - EAL7)

Evaluation Assurance Levels (EALs)

- Provide an increasing scale
- This scale attempts to balance:

  level of assurance obtained

  verses

  cost/feasibility of acquiring it

Things to Consider when Selecting an EAL

1. Value of the “assets”
2. Risk of the “assets” being compromised
3. Current state of practice
4. Development, evaluation, & maintenance costs
5. Resources of “adversaries”
6. Functional requirement dependencies
7. Security Objectives

EAL1 - Functionally Tested

- Applicable where IT-related risk is not a serious concern or where expectations toward the TOE are minimal
- No change to existing, commercial development practices
- Confidence in current operation is required
- No assistance from TOE developer
- Requirements:
  - Configuration Management: **ACM_CAP.1**
  - Delivery and Operation: **ACM_IGS.1**
  - Development: **ADV_FSP.1**, **ADV_RCR.1**
  - Guidance documents: **AGD_ADM.1**, **AGD_USR.1**
  - Tests: **ATE_IND.1**

EAL2: Structurally Tested

- Applicable where IT-related risk is not a serious concern or where the TOE is only expected to protect against less sophisticated threats
- No change to existing, commercial development practices
- Requires some cooperation of the developer
- Adds requirements for developer testing, vulnerability analysis, and more extensive independent testing
- Requirements:
  - Configuration Management: **ACM_CAP.2**
  - Delivery and Operation: ADO_IGS.1**, ADO_DEL.1**
  - Development: ADV_FSP.1, ADV_RCR.1, **ADV_HLD.1**
  - Guidance documents: AGD_ADM.1, AGD_USR.1
  - Tests: **ATE_IND.2, ATE_COV.1, ATE_FUN.1**
  - Vulnerability assessment: **AVA_SOF.1, AVA_VLA.1**

EAL3: Methodically Tested and Checked

- Applicable where concern for IT-related risks is greater, yet the expectations toward the TOE are still low
- No substantial changes in existing, commercial development practices
- Requires cooperation of the developer
- Places additional requirements on testing, development environment controls and configuration management
- Requirements:
  - Configuration Management: **ACM_CAP.3**, **ACM_SCP.1**
  - Delivery and Operation: ADO_DEL.1, ADO_IGS.1,
  - Development: ADV_FSP.1, ADV_RCR.1, **ADV_HLD.2**
  - Guidance documents: AGD_ADM.1, AGD_USR.1
  - Life Cycle support: **ALC_DVS.1**
  - Tests: **ATE_IND.2**, **ATE_COV.2**, **ATE_DPT.1**, ATE_FUN.1
  - Vulnerability assessment: AVA_SOF.1, AVA_VLA.1, **AVA_MSU.1**

EAL4: Methodically Designed, Tested, and Reviewed

- Applicable where concern for IT-related risks is moderate, yet the expectation for protection by the TOE is still limited
- Some security engineering added to commercial development practices
- Highest level likely for retrofit of an existing product
- Additional requirements on design, implementation, vulnerability analysis, development and configuration management
- Requirements:
  - Configuration Management: **ACM_CAP.4**, **ACM_SCP.2**, **ACM_AUT.1**
  - Delivery and Operation: **ADO_DEL.2**, ADO_IGS.1
  - Development: **ADV_FSP.2**, ADV_RCR.1, ADV_HLD.2, **ADV_IMP.1**, **ADV_LLD.1, ADV_SPM.1**
  - Guidance documents: AGD_ADM.1, AGD_USR.1
  - Life Cycle support: ALC_DVS.1, **ALC_LCD.1**, **ALC_TAT.1**
  - Tests: ATE_IND.2, ATE_COV.2, ATE_DPT.1, ATE_FUN.1
  - Vulnerability assessment: AVA_SOF.1, **AVA_VLA.2**, **AVA_MSU.2**

EAL5: Semiformally Designed and Tested

- Applicable where concern for IT-related risks is high and the TOE is expected to provide protection against sophisticated threats
- Application of security engineering to produce a product demonstrably resistant to penetration
- Additional requirements on specification, design, and their correspondence
- Requirements:
  - Configuration Management: ACM_CAP.4, **ACM_SCP.3**, ACM_AUT.1
  - Delivery and Operation: ADO_DEL.2, ADO_IGS.1
  - Development: **ADV_FSP.3**, **ADV_RCR.2**, **ADV_HLD.3**, **ADV_IMP.2**, ADV_LLD.1, **ADV_INT.1,ADV_SPM.3**
  - Guidance documents: AGD_ADM.1, AGD_USR.1
  - Life Cycle support: ALC_DVS.1, **ALC_LCD.2**, **ALC_TAT.2**
  - Tests: ATE_IND.2, ATE_COV.2, **ATE_DPT.2**, ATE_FUN.1
  - Vulnerability assessment: AVA_SOF.1, **AVA_VLA.3**, AVA_MSU.2, **AVA_CCA.1**

EAL6: Semiformally Verified Design and Tested

- Applicable where concern for IT-related risks is high and the TOE is expected to protect against sophisticated threats
- Application of rigorous security engineering to produce a product demonstrably resistant to penetration
- Additional requirements on analysis, design, development, configuration management, vulnerability/covert channel analysis
- Requirements:
  - Configuration Management: **ACM_CAP.5**, ACM_SCP.3, **ACM_AUT.2**
  - Delivery and Operation: ADO_DEL.2, ADO_IGS.1
  - Development: **ADV_FSP.3**, ADV_RCR.2, **ADV_HLD.4**, **ADV_IMP.3**, **ADV_LLD.2**, **ADV_INT.2,** ADV_SPM.3
  - Guidance documents: AGD_ADM.1, AGD_USR.1
  - Life Cycle support: **ALC_DVS.2**, ALC_LCD.2, **ALC_TAT.3**
  - Tests: ATE_IND.2, **ATE_COV.3**, ATE_DPT.2, **ATE_FUN.2**
  - Vulnerability assessment: AVA_SOF.1, **AVA_VLA.4**, **AVA_MSU.3**, **AVA_CCA.2**

EAL7: Formally Verified Design and Tested

- Applicable where concern for IT-related risks is very high and the TOE is expected to protect against sophisticated threats
- Application of rigorous security engineering and formal methods to produce a product demonstrably resistant to penetration
- Additional requirements for testing and formal analysis
- Requirements:
  - Configuration Management: ACM_CAP.5, ACM_SCP.3, ACM_AUT.2
  - Delivery and Operation: **ADO_DEL.3**, ADO_IGS.1
  - Development: **ADV_FSP.4**, **ADV_RCR.3**, **ADV_HLD.5**, ADV_IMP.3, ADV_LLD.2, **ADV_INT.3,** ADV_SPM.3
  - Guidance documents: AGD_ADM.1, AGD_USR.1
  - Life Cycle support: ALC_DVS.2, **ALC_LCD.3**, ALC_TAT.3
  - Tests: **ATE_IND.3**, ATE_COV.3, **ATE_DPT.3**, ATE_FUN.2
  - Vulnerability assessment: AVA_SOF.1, AVA_VLA.4, AVA_MSU.3, AVA_CCA.2

Augmentation

- Tailor existing Evaluation Assurance Levels (EALs)

Strength of TOE Security Functions (AVA_SOF)

- AVA_SOF.1 is included in EAL2 and higher
- For all TOE security functions realized by a probabilistic or permutational mechanism, a minimum SOF level must be chosen:
  - SOF-basic
  - SOF-medium
  - SOF-high
- FIA_SOS at EAL2 or higher requires an SOF level

Assurance Drills

Stages of Evaluation

- PP Evaluation: APE Class
- ST Evaluation: ASE Class
- TOE Evaluation: uses evaluated ST as the basis for evaluation

- Common Methodology for Information Technology Security Evaluation (CEM)

Protection Profiles

- Answers the question:

  "What do I want or need."

- Implementation Independent

- Who writes protection profiles:
  - **users -** anyone who has IT security needs, e.g., commercial consumer, consumer groups
  - vendors - anyone who supplies products which support IT security needs
  - others...

PP Contents

- Identification
- Overview
- TOE Description
- Security Environment
  - Assumptions
  - Policies
  - Threats
- Security Objectives
- Requirements
- PP Rationale

Class APE: Evaluation of Protection Profiles

- APE_DES - TOE Description
- APE_ENV - Security Environment
- APE_OBJ - Security Objectives
- APE_REQ - IT Security Requirements
- APE_SRE - Explicitly Stated IT Security Requirements
- APE_INT - PP Introduction

Security Targets

- Makes the statement: “This is what I have.”
- Implementation Dependent
- Vendors, developers write Security Targets

ST Contents

- Identification
- Overview
- TOE Description
- Security Environment
- Security Objectives
- Requirements
- **TOE Summary Specification**
- **PP Claims**
- Rationale

Class ASE: Evaluation of Security Targets

- ASE_DES - TOE Description
- ASE_ENV - Security Environment
- ASE_INT - Introduction
- ASE_OBJ - Security Objectives
- **ASE_PPC - PP Claims**
- ASE_REQ - IT Security Requirements
- ASE_SRE - Explicitly Stated IT Security Requirements
- **ASE_TSS - TOE Summary Specification**

Workshop Schedule
Wednesday

- 8am - 9am: Walk-through of a sample PP
- 9am - 10am: Threat Analysis Review
- 10am - noon: Mini-Threat Analysis Exercise
- 12pm - 1pm: Lunch
- 1pm - 2pm: Security Objectives Review
- 2pm - 4pm: Security Objective Development Exercise